Bridging the Cyberspace Gap

Washington and Silicon Valley

By Adam Segal

One of the defining characteristics of the cyber domain is the dominance of the private sector. The majority of critical networks are privately owned and operated; more than 90 percent of American military and intelligence communications travel over privately owned backbone telecommunications networks. Many of the most talented hackers are in the private sector, and private security firms such as CrowdStrike, FireEye, and Cylance have taken an increasingly large public role in tracing cyberattacks to nation-states and other perpetrators. In addition, Alphabet, Amazon, Apple, Cisco, Facebook, IBM, Intel, and other companies drive innovation and the deployment of new technologies, especially in cutting-edge areas like artificial intelligence. For these reasons, strong ties to the technology sector are central to the U.S. Government's (USG) pursuit of its economic, diplomatic, and military strategic interests in cyberspace.

Until June 2013, there was an overlap of interests between Washington and Silicon Valley. There were, of course, political differences. The first generation of information and communication technology entrepreneurs had a strong libertarian bent, and saw policy as a distant concern, if not an outright impediment. Still, the two sides worked together to advocate for free speech and open access online, reduce international trade barriers, and promote the promises of the information technology revolution globally. They also had a strong interest in sharing threat intelligence and technical indicators from cyberattacks.

In June 2013, however, former National Security Agency (NSA) contractor Edward Snowden revealed U.S. intelligence gathering and cyber practices and operations, many of them targeted at U.S. internet platforms and software and hardware providers. During the Cold War, the United States targeted specialized networks and devices on a relatively limited set of targets used by the Soviet Union, China, and other adversaries. Today, military, government, commercial, and individual users all use the same commercially-sourced networks, computers, and devices. The data of terrorists, generals, foreign policymakers, or arms dealers are likely to travel along and be stored in commercial products, and as a result, Silicon Valley platforms are always going to be targets.

Motivated by a sense of betrayal, a commitment to an open internet, and economic interest, the technology companies have responded to the revelations by increasingly portraying themselves as global actors. Many

Mr. Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

tech officials have argued for a more expansive definition of cybersecurity that focuses on the needs of all users and companies, rather than a more narrow definition centered on U.S. national security. In 2017, technology companies generated an estimated 60 percent of their revenues overseas. With their revenue increasingly dependent on foreign markets, especially China, there is also a strong motivation for the tech firms to demonstrate their independence from the USG.

The gap between Washington and Silicon Valley has only increased since 2013 after a number of public disputes.[1] In December 2015, a terrorist killed 14 people in San Bernardino, California. The Federal Bureau of Investigation (FBI) sought a court order to unlock one of the terrorist's iPhones. Apple protested, and public opinion was sharply divided over the balance between privacy and security. In January 2017, more than 125 technology companies joined an *amicus curiae* brief opposing President Trump's first executive order, which temporarily blocked all refugees and denied entry to citizens of seven predominantly Muslim countries. Tech company executives also expressed disappointment with President Trump's decision to withdraw from the Paris climate agreement; Elon Musk, the founder of SpaceX and Tesla, withdrew from two business councils providing advice to the administration on economic issues. Further driving the wedge between Washington and Silicon Valley, in June and July of the year, exploits developed from vulnerabilities discovered by the NSA were used in two large scale cyberattacks—WannaCry and NotPetya—that victimized the commercial sector and private users around the world, with losses totaling close to $8 billion by July 2017.[2]

The challenge of closing the divide is made even more pressing by the combination of a more assertive Chinese cyber diplomacy, the globalization of Chinese technology giants, and China's position as a leading hub for artificial intelligence research and development. After many years of reacting to Washington's efforts to shape cyberspace, Beijing has promoted a vision of governance centered on cyber sovereignty. As described by President Xi at the 2015 World Internet Conference in Wuzhen, China, cyber sovereignty means "respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet."[3] This position contrasts sharply with the vision held by the United States and its partners of cyberspace as an open, global platform, and has been furthered by commercial diplomacy and participation in forging international technical standards.

The Souring Relationship

Numerous countries have reacted to the Snowden disclosures by promoting industrial policies that avoid U.S. infrastructure, pressing for concessions from American technology companies, forcing companies to store data locally, or supporting domestic competitors. The Brazilian Government, for example, pushed forward plans for a new, high-capacity, fiber-optic cable connecting the Brazilian city of Fortaleza to Lisbon, Portugal, so as to prevent routing internet traffic through Miami. Moscow blocked access to LinkedIn after it failed to store Russian users' data locally. India pressed Microsoft for discounts of an estimated $50 million so users could upgrade to Windows 10 after the WannaCry and Petya cyberattacks.[4] In particular, Beijing has introduced several industrial policies as well as a national cybersecurity law designed to reduce dependence on foreign technology companies and promote local firms.

The technology companies responded to the disclosures with public outrage and efforts to hold the USG at arm's length through technology, legal challenges, and norms entrepreneurship. During the past three years, Apple, Microsoft, WhatsApp, and other companies have rolled out end-to-end encryption on smartphone operating systems, messaging services, and other online communications products. Data is scrambled in these products through mathematical formulas that the device manufacturer or service provider cannot reverse and recover data even when presented with a lawful warrant.

The move to encryption means that law enforcement and, to a lesser extent, intelligence agencies are unable to access data, even with a court order. In a March 2017 speech, for example, former FBI Director James Comey noted that in the last quarter of 2016, the FBI received 2,000 devices, and it was unable to access the data on 1,200 of them.[5] FBI and Department of Justice (DOJ) officials began warning about "going dark"—being unable to access data even with a warrant due to technological constraints—and to question the motivations of the technology companies.

In the face of this challenge, some federal agencies have called on U.S. technology companies to provide the technological means to bypass encryption, known as exceptional access or creating backdoors. These demands are not limited to the United States. After a Briton drove his car into pedestrians and attacked a police officer in March 2017, Home Secretary Amber Rudd said that intelligence agencies should have access to encrypted messages sent on WhatsApp. "We do want them to recognize that they have a responsibility to engage with government, to engage with law enforcement agencies when there is a terrorist situation," Rudd told the *BBC*. A few months later, German Interior Minister Thomas de Maizière announced that the German Government was preparing a new law that would give the authorities the right to decipher and read encrypted messages.

Tech companies have consistently argued that it is not possible to create backdoors without compromising the security of all users. Hackers and states will soon find ways of exploiting back doors. Or as Apple Chief Executive Officer Tim Cook put it, "You can't have a back door in the software because you can't have a back door that's only for the good guys."[7] Supporters of strong encryption also argue that neither the USG nor the private sector have a monopoly on encryption tools and methods. According to a Harvard University study, two-thirds of the nearly nine hundred hardware and software products that incorporate encryption have been built outside the United States.[8] Even if U.S. companies built in back doors, criminals and terrorists could easily use products developed elsewhere.

The technology companies have also mounted legal challenges to the USG's ability to collect data. Soon after the Snowden disclosures, Google and Microsoft filed motions with DOJ to be allowed to disclose how many times they had been ordered to share data with FISA. Microsoft also refused to comply with a Department of Justice demand for data from an Irish Outlook email account belonging to a suspect in a narcotics case. Microsoft argued that the data, stored in Ireland, was outside of U.S. jurisdiction and that requests for the information should go to the Government of Ireland.

On the legislative front, AOL, Apple, Facebook, Google, Microsoft, and Yahoo supported the *USA Freedom Act* and other legislative efforts to end bulk metadata collection of U.S. phone and data records. The Act, which was passed in June 2015, shifted bulk telephony metadata from the government to telecoms or private third parties. The same companies started a public campaign demanding "sensible limitations" on the ability of government agencies to compel tech companies to disclose user data. The companies argued, "Governments should limit surveillance to specific known users for lawful purposes, and should not undertake bulk data collection of internet communications."[9]

Technology companies have also taken a lead in defining and developing new norms of state behavior in cyberspace. In February 2017, Brad Smith, chief legal officer of Microsoft, gave a speech at the RSA cybersecurity conference calling for a Digital Geneva Convention "that will commit governments to protecting civilians from nation-state attacks in times of peace." Smith noted that one of the defining characteristics of the digital age is that cyberspace is produced, owned, secured, and operated by the private sector, and so the targets in cyberwar are private property owned by civilians. As a result, the tech companies act as "first responders" to nation-state attacks. In addition to deploying technical solutions such as encryption to fight state hacking, Smith called for the companies to "commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."[10]

In the wake of the WannaCry ransomware attack, Microsoft also criticized the vulnerabilities equities process (VEP), the method through which the government decides whether to reveal vulnerabilities to the private sector or to hold on to them for intelligence gathering or offensive cyber operations. WannaCry, which encrypted data and held it captive until a ransom was paid, exploited a vulnerability that was allegedly developed by NSA and was offered online by a group known as Shadow Brokers. How this vulnerability and other tools made their way to Shadow Brokers, which is assumed to be a cover for Russian intelligence, is unknown.

Obama officials claimed that the default of the VEP, which involves representatives from the NSA, FBI, and Department of Homeland Security, is toward defense and disclosure. In a blog post in April 2014, then White House Cybersecurity Coordinator Michael Daniel revealed that the process considers nine criteria, including whether a vulnerability is found in core infrastructure and the likelihood that adversaries will find it. While disclosing a vulnerability might mean the U.S. forgoes "an opportunity to collect crucial intelligence that could thwart a terrorist attack," Daniel wrote, hoarding them also has risks. "Building up a huge stockpile of undisclosed vulnerabilities while leaving the internet vulnerable and the American people unprotected would not be in our national security interest."[11] In 2015, NSA Director Admiral Michael Rogers said the agency discloses 91 percent of the vulnerabilities it finds.[12]

Microsoft's Smith argued that the leaks of NSA exploits is evidence that the VEP process is broken and that the government cannot safely stockpile vulnerabilities. "An equivalent scenario with conventional weapons would be," according to Smith, "the U.S. military having some of its Tomahawk missiles stolen."[13] In response, he argues the government should no longer stockpile, sell, or exploit vulnerabilities, but should report them to vendors.

Beijing's Assertive Cyber Diplomacy

The rupture between Washington and Silicon Valley is occurring at a time when China is taking a more active role in shaping cyberspace, and Chinese firms are playing a central role in the next wave of innovation. Beijing's early cyber diplomacy efforts were essentially a defensive crouch. China worked to control the destabilizing influence of the internet and the free flow of information through domestic laws and the deployment of filtering and censorship technologies widely known as the Great Firewall. On the international level, Beijing complained about what it saw as the uneven distribution of internet resources and defended itself from Western, especially American, accusations of internet censorship.

Under President Xi Jinping, China has more actively promoted its own vision of cyberspace governance. In November 2014, China held its first World Internet Conference in Wuzhen, a historic town near Hangzhou, home to the headquarters of the Alibaba Group. The event was meant as a showcase for the Chinese internet economy. It was at the second Wuzhen conference in 2015, that President Xi delivered his comments concerning "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing."[14]

Beijing has also used trade and investment in information technology infrastructure as an economic and political tool; much of the current investment and trade occurs as part of the One Belt, One Road (OBOR) initiative, a development strategy focused on connectivity and cooperation between China and Eurasia. Official Chinese documents have also stressed the need to build an "information silk road" through cross-border optical cables and other communications trunk line networks, transcontinental submarine optical cable projects, and spatial (satellite) communication.[15]

Chinese firms have invested in nodes along the Belt and Road. China's state owned telecommunication companies are planning new operations in Africa and Southeast Asia. China Comservice, a subsidiary of China Telecom, announced the "Joint Construction of Africa's Information Superhighway between China and Africa" with investment amounting to $15 billion and a 150,000 kilometer optical cable covering 48 African countries.[16] Private companies have also been active. In 2016, Chinese telecom equipment maker ZTE agreed to take over Turkish company Netas Telekomünikasyon for up to $101.28 million in a deal that would expand its operations across key markets covered by OBOR. Alibaba executive chairman Jack Ma is an adviser to the Malaysian government on the digital economy, and Huawei, in cooperation with Telekom Malaysia, is setting up a regional data hosting center in the country.[17]

Attempts to Bridge the Gap

The Obama Administration scrambled to repair the damage with the private sector. Driving the outreach was a belief not only that cooperation between the two sides was necessary in cyberspace but also that the next wave of defense innovation would occur in the private sector, not federal labs. In the past, government research and development was the main driver of technologies critical to the second offset, such as precision-guided weapons, stealth, imaging and sensor technology, and electronic warfare. Robotics, artificial intelligence, and the other technologies that define the third offset, however, will come from the nexus of public-and private-sector research and development. As former director of the Defense Advanced Research Projects Agency Arati Prabhakar put it, the secret of success is "going to be to harness that commercial technology and to turn it into military capabilities much more powerful than anyone else."[18]

Soon after the Snowden revelations, President Obama appointed a team of lawyers and national security experts to review the balance between privacy and security as well as efforts to promote an open internet and pursue commercial interests. In December 2013, the President's Review Group on Intelligence and Communications Technologies issued 46 recommendations on how to reform surveillance, including curtailing spying on foreigners to instances "directed exclusively at protecting the national security interests of the United States and our allies." The Group also noted the importance of encryption to the economy and urged the USG not to "in any way subvert, undermine, weaken, or make vulnerable generally available commercial software."[19]

In January 2014, the White House released Presidential Policy Directive (PPD) 28 on signals intelligence activities. PPD 28 affirmed the uses of intelligence collected in bulk for only six categories of threat (espionage, terrorism, and proliferation of weapons of mass destruction, cybersecurity, attacks on U.S. or allied armed forces, and transnational criminal threats) and banned U.S. agencies from distributing information collected on foreign citizens to other foreign intelligence agencies without considering "the privacy interests of non-U.S. persons."[20] The Intelligence Community must also delete a foreigner's personal information after five years unless it is determined that the information has intelligence value. PPD 28 was meant as an olive branch to the United States' European allies, but was also important to the companies, as it relieved some of the pressure European privacy regulators were putting on U.S. companies.

Obama White House and Department of Defense (DOD) officials also made numerous trips to Silicon Valley. The President gave talks at Stanford University and SXSW, an Austin-based festival of technology, music, and media. Defense Secretary Ashton Carter made four trips to Silicon Valley in 15 months. None of his predecessors had made the trip in 20 years.[21] Carter also created new institutions to strengthen ties. The Defense Innovation Unit Experimental (DIUx) is intended to help the military better tap into commercial tech innovation through more agile contracting and procurement. While DIUx struggled at first with slow acquisition times, it has had more recent successes, investing, for example, in a startup working on small civilian radar satellites that the Pentagon hopes to use over North Korea.[22]

Secretary Carter also established in March 2016 a Defense Innovation Advisory Board, made up of leaders from technology companies outside of the traditional defense industries, to offer "advice on innovative and adaptive means to address future organizational and cultural challenges." Chaired by Alphabet Executive Chairman Eric Schmidt, the board recommended the appointment of a chief innovation officer, the creation of a center for artificial intelligence and machine learning, and embedding software development teams within key commands.[23]

Former U.S. Secretary of Defense Ashton Carter stands in front of the Facebook wall during his visit to the company headquarters in 2014. Before the visit, the Defense Secretary unveiled DOD's cyber strategy at Stanford University. (DOD/Clydell Kinchen)

What Happens Next?

Despite calling for a boycott of Apple and warning Amazon it would face antitrust investigations as a presidential candidate, Donald Trump quickly invited CEOs to a Tech Summit soon after his election in November 2016. The meeting reportedly discussed vocational education and the application of information technology (IT) to reducing government waste. In June 2017, Apple Chief Executive Officer Tim Cook and Amazon CEO Jeff Bezos were among 18 executives who attended a meeting sponsored by the newly established Office of American Innovation. The office, led by Jared Kushner, aims to modernize federal IT systems, reduce government spending on IT, and improve the cybersecurity of government networks. Secretary of Defense James Mattis has signaled that he will continue support of DIUx.

Still, the relationship, as noted above, remains contentious, and issues such as immigration and climate change continue to drive the wedge. Both sides need to be realistic about what can be achieved, so as to insulate themselves from wide swings of emotion from over exuberance to a sense of betrayal. It is important that both sides acknowledge that distrust is bound to endure for at least two reasons. First, the economic incentives for Apple, Facebook, Google, Microsoft, and others to protect the privacy of their global users and publicly oppose the USG are unlikely to change. Opportunities to work more closely with the USG will not outweigh the lure of foreign markets. Second, as noted above, the platforms of these same companies will remain the target of NSA and other intelligence agencies. Potential U.S. adversaries, along with terrorists, hackers, and criminals, use commercial software and hardware. The Trump Administration, however, has the opportunity to put the relationship back on firmer footing with actions in three areas: encryption; data localization; and reforms of the VEP.

The encryption debate is a Gordian knot, with national security policymakers avowing there is a technological fix and the tech community asserting the opposite. In July 2017, for example, Acting Assistant Attorney General for National Security Dana Boente told the Aspen Security Forum, "I'm sure we'll find some technological brilliance that will provide the necessary security but still allow the government to do it [access encrypted data]."[24] That technological solution is, however, not coming, and efforts to force exceptional access are likely to result in lengthy battles pitting civil rights organizations and tech companies against the government.

Instead of seeking backdoors, the Trump Administration can explore other avenues of access to data. Despite concerns about encrypted devices, the FBI and others now have the ability to access texts, emails, social networking sites, and other data stored in the cloud. There is also a wealth of data being created and collected by new types of sensors in our phones, cars, and household devices.[25] Prosecutors in Arkansas recently demanded, for example, the recordings of an Amazon Echo smart speaker as evidence in a murder case.

Another option is to bypass encryption by exploiting existing security flaws in software to gather data. Known as lawful hacking, this would give law enforcement agencies the ability to hack into a suspect's smartphone or computer with a court order, such as a warrant. This type of hacking is likely to be resource intensive, requiring the development and acquisition of vulnerabilities, and so should be restricted to terrorism, violent crime, large-scale narcotic trafficking, and other serious threats.[26] Germany has taken such an approach, authorizing the police to use malware in investigations.[27]

As a corollary, law enforcement and investigative agencies will have to increase their investment in technology and technical expertise. The FBI, for example, has only 39 staff members who deal with encryption and anonymization technologies (eleven of whom are agents), and only $31 million in funding for those activities.[28] Congress should also provide funding for the FBI to share its capabilities with state and local police, who do not have adequate technological resources.

A second, actionable area for cooperation is creating a framework to respond to growing international demands for access to data. China, India, Indonesia, Malaysia, Nigeria, South Korea, Russia, and Vietnam have passed or are considering regulations that would require user data to be stored locally. The push to keep data within national borders has been driven in part by widespread frustration with the time-consuming and confusing legal processes involved in acquiring data from U.S. companies, which are prohibited under the Electronic Communication Privacy Act (ECPA) from releasing users' communications to foreign governments or authorities without a warrant from a U.S. judge.

This means that if an Indian citizen, for example, uses a Microsoft messaging app to plan and execute a crime in Delhi with other Indian citizens, Microsoft cannot disclose the messages directly to the Indian authorities. Instead, the Indian police has to request assistance from DOJ to petition a U.S. judge to obtain the communications on behalf of India. This process, enabled by a mutual legal assistance treaty (MLAT), is opaque, time consuming, and challenging for foreigners unfamiliar with the U.S. justice system. An MLAT request generally takes ten months to process, and U.S. companies are often forced to choose between two countries' legal demands.

During the Obama Administration, the United States and United Kingdom negotiated an agreement that would allow U.K. law enforcement agencies to request stored data and live intercepts directly from U.S. service providers, as long as the warrants did not target U.S. citizens, legal permanent residents, or anyone physically present in the United States. The Justice Department also introduced legislation that would allow the President to negotiate agreements with other foreign countries in which U.S. firms could respond to local law enforcement demands for emails and other communications. The legislation amends ECPA and authorizes Facebook, Google, and other U.S. providers to disclose data and communication content only to foreign governments that adhere to baseline due process, human rights, and privacy standards. The Trump Administration should continue this effort and work with Congress to ensure its adoption. As the ECPA reform process progresses, the Department of Justice should

The USG will not, and should not disclose all vulnerabilities to the private sector. There are legitimate security, intelligence, and law enforcement reasons for the government to hold on to vulnerabilities, and potential U.S. adversaries will not release disclosures to the public. But officials can be more transparent about the criteria for holding on to vulnerabilities, standardize the process of evaluation, and publish an annual report on the VEP's operations.

streamline the MLAT process. There should be a standard template for MLAT requests so that foreign governments know exactly what information they must provide to expedite the process, and the forms automated and simplified.

Third, the Trump Administration could reform the VEP. The USG will not, and should not disclose all vulnerabilities to the private sector. There are legitimate security, intelligence, and law enforcement reasons for the government to hold on to vulnerabilities, and potential U.S. adversaries will not release disclosures to the public. But officials can be more transparent about the criteria for holding on to vulnerabilities, standardize the process of evaluation, and publish an annual report on the VEP's operations. The President may also want to consider an executive order that formalizes the VEP process.[29]

It will not be enough just to be active at home. Beijing may benefit from Washington's apparent turn inward to play a larger role in defining the rules of the international order in cyberspace. The preliminary U.S. position on renegotiating the North American Free Trade Agreement does include provisions to "secure commitments not to impose customs duties on digital products, prohibit forced data localization, and ban governments from mandating the review of source code."[30] The abandonment of the Trans-Pacific Partnership, however, is likely to weaken U.S. efforts to shape cyberspace for its commercial and security interests as countries look to China. In particular, the growing trend of data localization is something China may be able to exploit diplomatically and economically.

Conclusion

Without any progress on these issues, U.S. technology companies are likely to continue to try and carve out their own path. The private sector will respond to the administration with limited cooperation on information sharing, a greater focus on encryption and other technological solutions for defending their own networks, and individual deals with governments around the world to smooth access to technology.[31] Apple, for example, announced in July 2017 that it would open its first data center in China.[32]

There is, of course, a limit to how far the companies will go. Technology companies are not of one mind on all of these issues, and some firms will continue to work with the USG. Some of those who protest loudly will find areas to cooperate quietly. Perhaps most important, the USG, and DOD in particular, remains an important customer. Or as Terry Halvorsen, the former Chief Information Officer of the Pentagon, put it: "I spend $36.8 billion a year. That buys a lot of potential trust."[33] It is not in the U.S. interest, however, to see how far that trust can be stretched. Unless the two sides find some common areas of cooperation, the U.S. ability to shape cyberspace in the near term is bound to be limited. PRISM

Notes

[1] Adam Segal, *Rebuilding Trust Between Silicon Valley and Washington*, Council on Foreign Relations Special Report, January 2017, available at <https: //www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington>.

[2] Jack Stubbs and Matthias, "Ukraine scrambles to contain new cyber threat after 'NotPetya' attack," *Reuters*, July, 2017, available at <http://www.reuters.com/article/us-cyber-attack-ukraine-backdoor-idUSKBN19Q14P>.

[3] Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, December 16, 2015, available at <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml>.

[4] "India Presses Microsoft for Windows Discount in Wake of Cyber attacks," *CNBC*, June 30, 2017, available at <http://www.cnbc.com/2017/06/30/india-presses-microsoft-for-windows-discount-in-wake-of-cyber-attacks.html>.

[5] FBI Director James Comey keynote address at the first annual Boston Conference on Cyber Security, March 8, 2017, available at <https://www.c-span.org/video/?424885-2/director-comey-remarks-cybersecurity-conference>.

[6] Mark Scott, "In Wake of Attack, U.K. Officials to Push Against Encryption Technology," *New York Times*, available at <https://www.nytimes.com/2017/03/27/technology/whatsapp-rudd-terrorists-uk-attack.html?mcubz=0>; Kieran McCarthy, "Look Who's Joined the Anti-encryption Posse: Germany, Come on Down," *The Register*, June 15, 2017, available at <https://www.theregister.co.uk/2017/06/15/germany_joins_antiencryption_posse/>.

[7] David Kravets, "Apple CEO Tim Cook blasts encryption backdoors," *ArsTechnica*, October 20, 2015, available at <https://arstechnica.com/tech-policy/2015/10/apple-ceo-tim-cook-blasts-encryption-backdoors/>.

[8] Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," February 11, 2016, available at <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf>.

[9] "Global Government Surveillance Reform," Reform Government Surveillance, May 19, 2015, available at <https://www.reformgovernmentsurveillance.com>.

[10] Brad Smith, "The need for a Digital Geneva Convention," available at <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

[11] Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," available at <https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>.

[12] Sean Lyngass, "NSA chief says agency discloses '91 percent' of zero day bugs," *FCW*, November 9, 2015, <https://fcw.com/articles/2015/11/09/rogers-zero-days-nsa-lyngaas.aspx>.

[13] Brad Smith, "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack," available at <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#zKiyEOFe1dxIx1zB.99>.

[14] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference," Ministry of Foreign Affairs, December 12, 2016, available at <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml>.

[15] "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," Consulate-General of the PRC in Vancouver, April 4, 2015, available at<http://vancouver.china-consulate.org/eng/topic/obor/>.

[16] For more information please reference <http://www.ey.com/Publication/vwLUAssets/ey-china-go-abroad-4th-issue-2016-en/$FILE/ey-china-go-abroad-4th-issue-2016-en.pdf>.

[17] Lokman Mansor, "Jack Ma is Now an Adviser to Malaysian Government on Digital Economy," *New Strait Times*, November 4, 2016, available at <http://www.nst.com.my/news/2016/11/185930/jack-ma-now-adviser-malaysian-govt-digital-economy>.

[18] Mohana Ravindranath, "DOD's Current InfoSec Strategy Is 'Patch and Pray,'" Nextgov, October 1, 2015, available at <http://www.defenseone.com/ideas/2015/10 /dods-current-infosec-strategy-patch-and-pray/122457/?oref=d-river>.

[19] White House, Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, available at <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

[20] White House, Presidential Policy Directive—Signals Intelligence Activities, January 17, 2014, available at <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[21] Henny Sender, "U.S. Defense: Losing its edge in technology?" *Financial Times*, September 4, 2016, available at <https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907>.

[22] Dan Lamothe, "Pentagon Chief Overhauls Silicon Valley Office, Will Open Similar Unit in Boston," *Washington Post*, May 11, 2016, available at <https://www.washingtonpost.com/news/checkpoint/wp/2016/05/11/pentagon-chief-overhauls-silicon-valley-office-will-open-similar-unit-in-boston/?tid=a_inl-amp&utm_term=.669353214d20>; David Sanger and William Broad, "Tiny Satellites From Silicon Valley May Help Track North Korea Missiles," *New York Times*, July 6, 2017, available at <https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html>.

[23] U.S. Department of Defense, "Pentagon to Establish Defense Innovation Advisory Board," March 2, 2016, available at <https://www.defense.gov/News/Article/Article/684366/pentagon-to-establish-defense-innovation-advisory-board/>; Aaron Mehta, "Defense Innovation Board Lays Out First Concepts," *DefenseNews*, October 5, 2016, available at <http://www.defensenews.com/articles/defense-innovation-board-lays-out-first-concepts>.

[24] Morning Cybersecurity, July 24, 2017, available at <http://www.politico.com/tip-sheets/morning-cybersecurity/2017/07/24/will-the-us-follow-europe-on-encryption-221486>.

[25] "Don't Panic Making Progress on the 'Going Dark' Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, available at <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>.

[26] Susan Hennessey, "Lawful Hacking and the Case for a Strategic Approach to "Going Dark," Brookings, October 7, 2016, available at <https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/>.

[27] Joseph Cox, "Germany Just Gave Cops More Hacking Powers to Get Around Encryption," Motherboard, June 22, 2017, available at <https://motherboard.vice.com/en_us/article/gyp7em/germany-just-gave-cops-more-hacking-powers-to-get-around-encryption>.

[28] Robyn Greene, "Unbounded and Unpredictable," Open Technology Institute, New America, August 22, 2016, available at <https://www.newamerica.org/oti/blog/unbounded-and-unpredictable>.

[29] Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," Belfer Center for Science and International Affairs, June 2016, available at <http://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf>.

[30] U.S. Trade Representative, Summary of the Objectives for the NAFTA Renegotiation, July 17, 2017, available at <https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf>.

[31] Segal, *Rebuilding Trust*.

[32] Paul Mozur, "Apple Opening Data Center in China to Comply With Cybersecurity Law," *New York Times*, July 12, 2017, available at <https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html?mcubz=0>.

[33] Sara Sorcher, "Pentagon's Top IT Official: My Money Buys Silicon Valley's Trust," Passcode (blog), *Christian Science Monitor*, October 29, 2015, available at <http://www.csmonitor.com/World/Passcode/2015/1029/Pentagon-s-top-IT-official-My-money-buys-Silicon-Valley-s-trust>.